УДК 003.26.09

В. Ф. ГОЛИКОВ, В. Л. ПИВОВАРОВ

ПОВЫШЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ КРИПТОГРАФИЧЕСКОГО КЛЮЧА, СФОРМИРОВАННОГО В УСЛОВИЯХ УТЕЧКИ ИНФОРМАЦИИ О ЗНАЧЕНИИ НЕКОТОРОЙ ЕГО ЧАСТИ

Белорусский национальный технический университет

В статье рассматривается возможность повышения конфиденциальности криптографического ключа, сформированного в условиях утечки информации о значениях некоторой части ключа. Такая ситуация может сложиться при формировании общего криптографического ключа симметричной криптосистемы при использовании квантового канала, прослушиваемого криптоаналитиком, или другими методами, не использующими односторонние функции. Предлагается способ преобразования со случайными секретными параметрами сформированной ключевой последовательности, с помощью которого можно увеличить энтропию последней. Суть разработанной процедуры заключается в том, что абоненты A и B секретно от криптоаналитика, но согласовано между собой, выбирают некоторые биты в сформированной ключевой последовательности, (в дальнейшем называемые «помеченными»), а затем производят заранее объявленное преобразование этой последовательности, используя при этом информацию о помеченных битах.

Так как количество и порядковые номера помеченных битов неизвестны криптоаналитику, то и расположение известных ему ранее битов, изменяется случайным образом и становиться неопределенным. Принципиальным моментом этого способа является получение помеченных битов, номера которых известны только A и B, не используя для этого защищенный канал связи. Описывается один из возможных методов получения помеченных битов, основанный на случайном и независимым инвертировании сформированной ключевой последовательности абонентами A и B с последующим анализом четностей пар битов. Оценивается эффективность метода.

Ключевые слова: *криптографический ключ, утечка информации, секретное преобразование, повышение неопределенности.*

Введение

В современных технологиях защиты информации криптографические методы играют большую роль. Перспективным направлением в криптографии является использование квантовых эффектов. Так в задаче формирования общего криптографического ключа симметричной криптосистемы используют квантовый канал для передачи ключевой информации в виде одиночных фотонов. Одним из главных недостатков квантового способа формирования ключа является наличие возможности у криптоаналитика, подключившегося к квантовому каналу, узнать часть ключевой информации, в предельном случае до 25% [1]. В связи с этим широко известные классические протоколы [2, 3] запрещают использовать сеансы формирования ключа, если обнаружен факт «прослушивания» канала. Такое ограничение существенно сужает область применения классических протоколов, сводя ее к тривиальной ситуации – безопасный ключ может быть сформирован только при отсутствии «прослушивающего» криптоаналитика. Подобные утечки информации возникают и при других методах формирования общего криптографического ключа с использованием открытого канала связи [4, 5].

В статье рассматривается возможность повышения конфиденциальности криптографического ключа, сформированного в условиях утечки информации о значениях некоторой части ключа.

Постановка задачи

Пусть субъекты A и B, используя, например, квантовый канал передачи информации,

сформировали общую бинарную последовательность $X_{AB} = \{0, 1\}^{2n}$, где $2n$ – длина последовательности в битах (четное число). Криптоаналитику E, прослушавшему квантовый канал, известно d битов $(0 \le d << n)$. A и B знают об этом, но им неизвестно, количество и какие биты ключа известны E. Требуется сформировать криптографический ключ K_{AB} длиной n, $n \le 2n$, неопределенность которого, если ее измерять энтропией, равнялась бы $H_K \ge 2n - d$.

Решение

Предлагается способ преобразования со случайными секретными параметрами исходной ключевой последовательности X_{AB} в K_{AB}, с помощью которого можно увеличить энтропию последнего. Суть разработанной процедуры заключается в том, что A и B секретно от E, но согласовано между собой, выбирают некоторые биты случайным образом в последовательности X_{AB}, (в дальнейшем будем их называть «помеченными»). Затем производят заранее объявленное преобразование последовательности X_{AB}, используя при этом информацию о помеченных битах.

Так как количество и порядковые номера помеченных битов неизвестны E, то и расположение известных ему ранее d битов, изменяется случайным образом и становиться неопределенным. Принципиальным моментом этого способа является получение помеченных битов, номера которых известны только A и B, не используя для этого защищенный канал связи.

Рассмотрим основные этапы предлагаемого способа.

1. A и B случайным образом независимо и секретно друг от друга, а также от E, инвертируют $2r$ битов в своих последовательностях X_{AB}, $r \le n$.

2. A и B разбивают полученные после инвертирования последовательности X_A и X_B на фрагменты по два бита в каждом и вычисляют четности каждой пары:

$$C_i^A = a_j \oplus a_{j+1},\ C_i^B = b_j \oplus b_{j+1},$$

где $C_i^A = \{0,1\}$, $C_i^B = \{0,1\}$ – четности i-той пары соответственно X_A, X_B; a_j, b_j – биты i-той пары соответственно в X_A, X_B; i – номер пары, $i = \overline{1,n}$; j – номер бита в i-той паре, $j = 2i - 1$, $j = \overline{1,2n}$. При этом $a_j = b_j$, если оба бита не инвертированы или оба бита инвертированы; $a_j = 1 - b_j$, если один из битов инвертирован.

3. A и B сообщают друг другу по открытому каналу связи четности своих последовательностей C_i^A, C_i^B.

4. A и B производят сравнение четностей своей последовательности с четностями последовательности партнера, т. е. C_i^A сравнивается с C_i^B для каждого i. В результате такого сравнения каждый субъект определяет номера пар, для которых выполняется: $C_i^A \ne C_i^B$ или $C_i^A \ne C_i^B$.

Равенство четностей возникает в результате следующих событий:

1. В i-тых парах A и B все четыре бита не инвертированы, либо инвертированы:

$$(a_j, a_{j+1}), (b_j, b_{j+1}) \text{ или } (\overline{a_j}, \overline{a_{j+1}}), (\overline{b_j}, \overline{b_{j+1}}).$$

2. В каждой i-той паре A и B инвертировано по одному биту безразлично какому:

$$(\overline{a_j}, a_{j+1}), (\overline{b_j}, b_{j+1}) \text{ или } (\overline{a_j}, a_{j+1}), (b_j, \overline{b_{j+1}}), \ldots$$

Неравенство четностей возникает в результате следующих событий:

В i-той паре одной из последовательностей инвертирован только один бит, безразлично какой, а в i-той паре другой последовательности инвертировано оба бита или ни одного:

$$(\overline{a_j}, a_{j+1}), (\overline{b_j}, \overline{b_{j+1}})$$

или

$$(\overline{a_j}, a_{j+1}), (b_j, b_{j+1}), \ldots$$

3. A и B из всех пар выбирают пары, для которых $C_i^A = C_i^B$, а из них те пары, в которых инвертировано только по одному биту, рассуждая следующим образом «… я знаю, что в моей паре инвертирован только один бит, а четность этой пары совпадает с четностью пары партнера, значит и в его паре инвертирован только один бит…». Рассуждая аналогично, второй субъект тоже выбирает эти же пары. Криптоаналитик не знает какие биты были инвертированы в X_A и X_B, поэтому не может распознать выбранные A и B пары, несмотря на то, что четности пар ему известны. Пары, относящиеся к группе *1* и *2*, для криптоаналитика неразличимы по их четностям. Выбранные пары в дальнейшем будем называть помеченными.

4. A и B проводят некоторое заранее оговоренное преобразование (известное E) своих последовательностей X_A и X_B, (например, пере-

становки), используя при этом значения битов из помеченных пар, их порядковые номера j, количество помеченных пар. В результате такого преобразования порядковые номера битов исходной последовательности X_{AB} изменяются. Так как количество и порядковые номера помеченных бит случайны, то конечная последовательность случайным образом отличается от исходной, а знания криптоаналитика E о d битах исходной последовательности из детерминированной информации превращаются в вероятностную.

5. A и B производят обратное инвертирование своих последовательностей.

Исследование эффективности

Самостоятельный интерес представляют анализ криптостойкости конечного ключа, ее зависимость от возможных стратегий криптоаналитика, от выбора параметров n, r и значения d. Криптоаналитику E известно: d, n, r, а также C_i^A, C_i^B. Оценим его возможности по нахождению помеченных пар.

Знание четностей пар C_i^A, C_i^B, во-первых, позволяет E выбрать пары, которые потенциально могут оказаться помеченными. К таким относятся пары, для которых $C_i^A = C_i^B$. Поэтому желательно, чтобы количество таких пар было максимально возможным, чтобы затруднить в дальнейшем их перебор. Определим отчего зависит вероятность образования таких пар. Если из последовательностей X_A и X_B взять наугад по одной паре, то вероятность того что в каждой из них инвертирован один бит, равна

$$P_{A,B}(1,1) = P_A(1)P_B(1),$$

где $P_A(1)$, $P_B(1)$ – вероятность того что инвертирован один бит в паре из X_A, X_B соответственно. Очевидно, что $P_A(1) = P_B(1)$, поэтому ограничимся нахождением $P_A(1)$. Искомая вероятность равна

$$P_A(1) = P\left(a_j, \overline{a_{j+1}}\right) + P\left(\overline{a_j}, a_{j+1}\right) = 2\frac{r}{n}\left(1 - \frac{r}{n}\right).$$

Аналогично

$$P_B(1) = 2\frac{r}{n}\left(1 - \frac{r}{n}\right).$$

Следовательно,

$$P_{A,B}(1,1) = 4\frac{r^2}{n^2}\left(1 - \frac{r}{n}\right)^2 \qquad (1)$$

Выражение (1) имеет максимум, равный 1/2, при $r = 0{,}5n$. Таким образом, максимально возможное число помеченных пар равно половине общего числа пар.

Кроме того, выбор условия $r = 0{,}5n$ имеет дополнительное положительное влияние на неопределенность X_{AB}. Знание значения четности каждой пары криптоаналитиком, позволяет ему выдвигать гипотезы относительно значений битов в этих парах. Например, если $C_i^A = 0$, то вероятность того, что в X_{AB} биты этой пары одинаковы равна

$$P = P\left(a_j = a_{j+1}\right) + P\left(\overline{a_j} = \overline{a_{j+1}}\right) = \left(1 - \frac{r}{n}\right)^2 + \frac{r^2}{n^2}.$$

При $r = 0{,}5n$ вероятность $P = 1/2$, что делает гипотезу о равенстве битов в паре и гипотезу о противоположности этих битов равновероятными. Таким образом, при $r = 0{,}5n$ знание C_i^A и C_i^B не может быть использовано E.

Будем оценивать криптостойкость ключа по отношению полному перебору его значений.

Поскольку после проделанного случайного преобразования X_{AB} в K_{AB}, криптоаналитик E не знает местоположение известных ему ранее битов, то для него объем полного перебора K_{AB} равен $M_k = 2^{2n}$. Однако, зная алгоритм преобразования с точностью до количества помеченных битов и их номеров, E может использовать свои знания о d битах исходного ключа X_{AB}, используя для этого следующую стратегию.

E последовательно выдвигает гипотезы о количестве помеченных битов и проверяет их учитывая пары, которые не могут быть помеченными, осуществляя полный перебор значений оставшихся бит, исключая из него d известных ему битов.

Например, пусть $2n = 12$,

$$X_{AB} = a_1 a_2\, a_3 a_4\, a_5 a_6\, a_7 a_8 a_9 a_{10} a_{11} a_{12}.$$

A и B инвертируют в X_{AB} по 6 битов $(2r = 6)$:

$$X_A = a_1 a_2 \overline{a_3} a_4 \overline{a_5} a_6\, a_7 \overline{a_8}\, \overline{a_9}\, \overline{a_{10}} a_{11} a_{12},$$

$$X_B = \overline{a_1}\,\overline{a_2}\, a_3 \overline{a_4}\, a_5 a_6 \overline{a_7} a_8 \overline{a_9} a_{10} \overline{a_{11}} a_{12}.$$

Сравнивая четности пар с одинаковыми порядковыми номерами получим:

$$C_1^A = C_1^B,\ C_2^A = C_2^B,\ C_3^A \neq C_3^B,$$

$$C_6^A \neq C_6^B,\ C_6^A \neq C_6^B,\ C_6^A \neq C_6^B.$$

Для A и B помеченными парами являются пары с номерами: 2, 4. В качестве преобразования используем изъятие помеченных пар и размещение первого бита пары на первой позиции, второго на последней. Получим:

$$X_A = a_7 \overline{a_3} a_1 a_2 \overline{a_5} a_6 \overline{a_9}\,\overline{a_{10}} a_{11} a_{12} a_4 \overline{a_8},$$

$$X_B = \overline{a_7}\, a_3 a_1 \overline{a_2}\, a_5 a_6 \overline{a_9} a_{10} \overline{a_{11}} a_{12} \overline{a_4} a_8.$$

После обратного инвертирования A и B имеют одинаковый ключ

$$K_{AB} = a_7\, a_3 a_1 a_2\, a_5 a_6 a_9 a_{10} a_{11} a_{12} a_4 a_8.$$

Пусть E знает три бита $d = 3$, т. е. для него X_{AB} представляется как

$$X_E = x_1 a_2 x_3 x_4 x_5 a_6 x_7 x_8 x_9 a_{10} x_{11} x_{12},$$

где $x_1, x_3, x_4, x_5, x_7, x_8 x_9 x_{10} x_{12}$ – неизвестные для E биты.

Криптоаналитик E знает, что пары с номерами 3, 5, 6 не могут быть помеченными.

E выдвигает гипотезу H_0: в X_{AB} помечено 0 пар. Этой гипотезе соответствует последовательность K_{AB}, равная:

$$x_1 a_2 x_3 x_4 x_5 a_6 x_7 x_8 x_9 a_{10} x_{11} x_{12}.$$

E выдвигает гипотезу H_1: в X_{AB} помечена 1 пара: Этой гипотезе соответствуют последовательности K_{AB}, равные:

$$x_1 x_3 x_4 x_5 a_6 x_7 x_8 x_9 a_{10} x_{11} x_{12} a_2;$$

$$x_3 x_1 a_2 x_5 a_6 x_7 x_8 x_9 a_{10} x_{11} x_{12} x_4,$$

$$x_7 x_1 a_2 x_3 x_4 x_5 a_6 x_9 a_{10} x_{11} x_{12} x_8.$$

E выдвигает гипотезу H_2: в X_{AB} помечено 2 пары. Этой гипотезе соответствуют последовательности K_{AB}, равные:

$$x_9 x_1 x_3 x_4 x_5 a_6 x_7 x_8 x_{11} x_{12} a_2 a_{10};$$

$$x_9 x_1 x_3 x_4 x_5 a_6 x_7 x_8 x_{11} x_{12} a_2 a_{10};$$

$$x_9 x_3 x_1 a_2 x_5 a_6 x_7 x_8 x_{11} x_{12} x_4 a_{10}.$$

E выдвигает гипотезу H_3: в X_{AB} помечено 3 пары. Этой гипотезе соответствуют последовательности K_{AB}, равные:

$$x_9 x_4 x_1 x_3 a_6 x_7 x_8 x_{11} x_{12} a_2 x_5 a_{10}.$$

Таким образом, перебор неизвестных значений элементов ключа при трех гипотезах равен соответственно: C_1^3, C_1^3, C_2^3, C_3^3. С учетом неизвестных E бит $x_1, x_3, x_4, x_5, x_7, x_8, x_9, x_{10}, x_{11}$ полный перебор значений K_{AB} будет равен $M = (C_0^3 + C_1^3 + C_2^3 + C_3^3)2^9 = 2^{12}$.

Суммарный объем перебора для E при данной стратегии оказался таким же, что и перебор всех значений X_E без использования своих априорных знаний $M = M_K$, где $M_K = 2^{12}$. Однако, надо иметь ввиду, что, во-первых, вероятности перечисленных гипотез различны, т. е. в конечном итоге эффективность рассматриваемой стратегии будет зависеть от вероятностных характеристик количества помечаемых бит. В связи с этим целесообразно исследовать статистические свойства числа помечаемых пар. Найдем распределение вероятностей числа помечаемых пар.

Согласно приведенному выше алгоритму в последовательностях X_A и X_B помечается пара, в которой оказался один инвертированный бит. Обозначим число таких пар через S. Очевидно, что S зависит от количества пар в последовательностях X_A и X_B, содержащих один инвертированный бит. Обозначим число таких пар через R_A и R_B. Таким образом имеем систему случайных величин (S, R_A, R_B). Обозначим распределение вероятностей этой системы как $P(S = s, R_A = r_A, R_B = r_B)$. Так как S зависит от R_A и R_B, то справедливо:

$$P(s, r_A, r_B) = P(s|r_A, r_B)\, B(r_A, r_B),$$

где $P(s|r_A, r_B)$ – условная вероятность. Так как R_A и R_B независимые случайные величины, то получим:

$$P(s, r_A, r_B) = P(s|r_A, r_B)\, P(r_A)\, P(r_B). \qquad (2)$$

Вероятность числа помеченных пар получим интегрированием (1) по r_A и r_B

$$P(s) = \sum_{r_A = f(s)} \sum_{r_B = f(s, r_A)} P(s|r_A, r_B) P(r_A) P(r_B), \quad (3)$$

где $f(s)$, $f(s, r_A)$ – области интегрирования, учитывающие связи между переменными r_A, r_B, s. Найдем составляющие (3). Начнем с определения $P(r_A)\, P(r_B)$.

Процесс образования r_A и r_B идентичен, поэтому для упрощения обозначений рассмотрим его исходя из следующей постановки задачи. Имеется бинарная случайная последовательность длиной $2n$, в ней случайным образом инвертировано $2r$ битов. В результате этого образовалось: R_0 пар без инвертированных бит (a_j, a_{j+1}); R_1 пар с одним инвертированным битом, причем из них R_{01} пар содержат в паре биты, расположенные в порядке (a_j, $1 - a_{j+1}$), R_{10} пар содержат в паре биты, расположенные в порядке ($1 - a_j$, a_{j+1}), R_2 пар с двумя инвертированными битами ($1 - a_j$, $1 - a_{j+1}$).

Система случайных величин (R_0, R_{01}, R_{10}, R_2) имеет полиномиальное распределение $P(R_0 = r_0, R_{01} = r_{01}, R_{10} = r_{10}, R_2 = r_2)$ с коэффициентами

$$\frac{n!}{r_0!r_{01}!r_{10}!r_2!}. \quad (4)$$

Учитывая связи между рассматриваемыми величинами можно записать следующие соотношения:

$$\begin{cases} r_{01} + r_{10} = r_1 \\ r_0 + r_1 + r_2 = n \\ r_1 + 2r_2 = r \end{cases} \quad (5)$$

Тогда (4), можно записать как

$$\frac{n!}{\left(n - r - \frac{r_1}{2}\right)!\,(r_1 - r_{10})!\,r_{10}!\left(r - \frac{r_1}{2}\right)!}. \quad (6)$$

Знание этих коэффициентов позволит найти распределение вероятностей случайной величины R_1 (а это R_A или R_B), как отношения количества значений бинарной последовательности $M(r_1)$ при которых $R_1 = r_1$

$$M(r_1) = \sum_{r_{10}=0}^{r_1} \frac{n!}{\left(n - r - \frac{r_1}{2}\right)!\,(r_1 - r_{10})!\,r_{10}!\left(r - \frac{r_1}{2}\right)!} \quad (7)$$

к общему количеству возможных значений бинарной последовательности M

$$M = \sum_{r_1=0}^{2r} \sum_{r_{10}=0}^{r_1} \frac{n!}{\left(n - r - \frac{r_1}{2}\right)!\,(r_1 - r_{10})!\,r_{10}!\left(r - \frac{r_1}{2}\right)!}. \quad (8)$$

Следует иметь в виду, что r_1 может принимать только четные значения, поскольку общее число инвертированных бит $2r$ четное число. Максимально возможное значение r_1 равно $2r$.

Можно показать, что величина M равна $\binom{2N}{2r}$. Тогда искомая вероятность равна

$$P(R_1 = r_1) = \frac{M(r_1)}{\binom{2N}{2r}}.$$

Таким образом, окончательно имеем

$$P(r_A) = P(r_B) = \frac{M(r_1)}{\binom{2n}{2r}}. \quad (9)$$

Вероятность $B(s|r_A, r_B)$ – это вероятность того, что, если в последовательностях X_A и X_B соответственно образовалось R_A и R_B пар с одним инвертированным битом, то число таких совпадающих пар будет S. Вычислим эту вероятность по аналогии с [6]. Если в последовательности X_A содержится r_A пар типа r_1, то число возможных комбинаций, в которых из r_B пар типа R_1 s пар совпадает с аналогичными парами из R_A, равно $\binom{r_A}{s}\binom{n - r_A}{r_B - s}$. Так как сама последовательности X_A может принимать $\binom{n}{r_A}$ значений, то общее число значений X_A и X_B в которых совпадает s пар типа R_1 равно $M(s) = \binom{r_A}{s}\binom{n - r_A}{r_B - s}\binom{n}{r_A}$. Общее же число всевозможных комбинаций равно $M = \binom{n}{r_A}\binom{n}{r_B}$, тогда искомая вероятность равна

$$P(s|r_A, r_B) = \frac{\binom{r_A}{s}\binom{n - r_A}{r_B - s}}{\binom{n}{r_B}}. \quad (10)$$

Имея все составляющие (1), окончательно можно записать

$$P(s) = \sum_{r_A = f(s)} \sum_{r_B = f(s, r_A)} \frac{\binom{r_A}{s}\binom{n - r_A}{r_B - s}}{\binom{n}{r_B}} \times$$

$$\times \left\{ \frac{\sum_{r_{10}=0}^{r_A} \frac{n!}{\left(n - r - \frac{r_A}{2}\right)!\,(r_A - r_{10})!\,r_{10}!\left(r - \frac{r_A}{2}\right)!}}{\binom{2n}{2r}} \times \right.$$

$$\left. \times \frac{\sum_{r_{10}=0}^{r_B} \frac{n!}{\left(n - r - \frac{r_B}{2}\right)!\,(r_B - r_{10})!\,r_{10}!\left(r - \frac{r_B}{2}\right)!}}{\binom{2n}{2r}} \right\}. \quad (11)$$

Суммирование в (11) должно вестись с учетом того, что величины r_A и r_B принимают только четные значения 0, 2, 4, …, $2r$, а также условия: $\min(r_A, r_B) \geq s \geq \max(0, r_A + r_B - n)$. По-

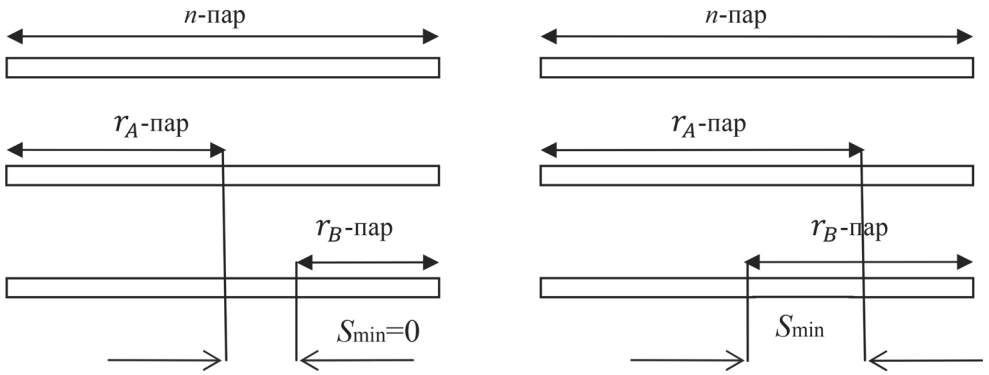
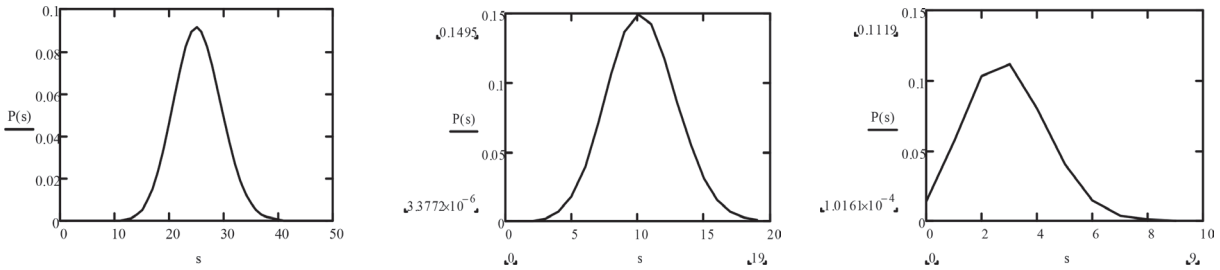


Рис. 1. Границы величины S



а *б* *в*

Рис. 2. Распределение вероятностей для $n = 100$ при $r = 50$, $r = 20$, $r = 10$

следнее условие вытекает из того, что с одной стороны число совпадающих пар не может быть больше, чем минимальное число пар типа r_1 в одной из последовательностей, а с другой, если суммарное значение числа совпадающих пар обеих последовательностей превосходит общее число пар, то минимальное значение s не может быть меньше, чем величина превышения (рис. 1). Распределение вероятностей (11) изображено на рис. 2 для $n = 100$ при $r = 50$, $r = 20$, $r = 10$ соответственно. Из рисунков видно, что число битов, их порядковые номера, помечаемые сторонами A и B секретно от E, зависят от числа инвертированных битов r и колеблются в достаточно широком диапазоне, что затрудняет криптоанализ сформированного ключа методом полного перебора. Так, например, если криптоаналитик попытается перебрать все возможные варианты с помеченными парами при $n = 100$ и $r = 50$, ограничив возможный диапазон значений S наиболее вероятным [20, 30], то количество вариантов составит примерно 10^{25}.

Заключение

Предложенный способ повышения конфиденциальности криптографического ключа, сформированного в условиях утечки информации о значениях некоторой его части позволяет существенно затруднить попытку вычисления его значения полным перебором, если речь идет о ключе блочного алгоритма шифрования, и не допустить расшифрования части зашифрованного сообщения, если утечка произошла в системе поточного шифрования. Открытым остается вопрос о выборе вида преобразования, использующего помеченные пары битов.

Литература

1. **Bennet, C. H. Brassard, G.** Quantum cryptography: quantum key distribution and coin tossing/ Int. conf. on computers systems ans signal processing. – Bangalore, 1984. P. 175–179.

2. **Брассар Ж.** Современная криптология. – М.: Полимед, 1999. – 178с.

3. **Боумейстер, Д.** Физика квантовой информации. / Д. Боумейстер, А. Экерт, А. Цайлингер. – М.: Постмаркет, 2002. – 276с.

4. **Способ** распределения криптографического ключа между абонентами: пат. 17856 Респ. Беларусь: МПК 04L 9/08 (2006.01) / В. Ф. Голиков; дата публ.: 19.07.2011.

5. **Голиков, В. Ф.** Оценка потерь конфиденциальности при неклассических способах формирования криптографического ключа / В. Ф. Голиков, Ф. Абдольванд // Информатика.– 2011. –№ 2 (30). – С. 104–110.

6. **Беляев, Ю. К.** Вероятностные методы выборочного контроля. – М.: изд. Наука,1975.– 407с.

References

1. **Bennet, C. H. Brassard, G.** Quantum cryptography: quantum key distribution and coin tossing/ Int. conf. on computers systems ans signal processing. – Bangalore, 1984. P. 175–179.
2. **Brassar, J.** Modern cryptology. – M.: Polymed, 1999. – 178 p.
3. **Baumeister, D.** The physics of quantum information. / D. Baumester, A. Ekert, A. Tsailinger. –M:. Postmarket, 2002. – 276 p.
4. **Method** of cryptographic key distribution between subscribers: pat. 17856 Rep. Belarus: IPC 04L 9/08 (2006.01) / V. F. Golikov; date publ.: 19.07.2011.
5. **Golikov, V. F.** Estimation of loss of confidentiality of non-classical methods of forming a cryptographic key / V. F. Golikov, F. Abdolvand // Informatika. – 2011. – № 2 (30). – P. 104–110.
6. **Belyaev, Y. K.** Probabilistic methods of sampling. – M.: Science, 1975. – 407 p.

Поступила	*После доработки*	*Принята к печати*
03.05.2016	*15.05.2016*	*20.05.2016*

Holikau U. F., Pivovarov V. L.

CRYPTOGRAPHIC KEY IMPROVED PRIVACY UNDER THE CONDITIONS OF SOME OF CRYPTOGRAPHIC KEY VALUE DATA LEAK

Belarusian National Technical University

The article outlines the possibility of increasing the privacy of cryptographic key generated in the conditions of data leakage of some of its values. Such a situation can occur in the formation of a common cryptographic key of a symmetric cryptosystem employing a quantum channel, listened by a cryptanalyst, or other methods that do not make use of one-way functions. A method with the conversion parameters to increase the entropy of a generated secret random key sequences suggested. The essence of the procedure developed is that the subscribers A and B (secretly to a cryptanalyst), but in agreement with each other, choose some of the bits in the generated key sequence (further referred to as «tagged») and produce a pre-announced conversion of this sequence, using the data about the tagged bits.

Since the amount and serial numbers of tagged bits are unknown to a cryptanalyst, the layout of the bits known to a cryptanalyst before randomly changes and becomes uncertain. The fundamental point of this method is to obtain tagged bits, the positions of which are known only to subscribers A and B without using the secure communication channel. One of the possible methods of obtaining tagged bits based on a random and independent inversion of a generated key sequence by the subscribers A and B and followed by the analysis of parities pairs of bits is analyzed. The efficiency of the method is evaluated.

Keywords: *cryptographic key, dataleak, secret conversion, increased uncertainty.*

Голиков Владимир Федорович

Доктор технических наук, профессор. Заведующий кафедрой «Информационные технологии в управлении» Белорусского национального технического университета. Сфера научных интересов: защита информации, криптография.

E-mail: vgolikov@bntu.by

Пивоваров Вадим Леонидович

В 2012 окончил Белорусский Государственный Университет по специальности «Информатика». Аспирант Белорусского национального технического университета, специалист по программированию на языке C#. Соавтор трех научных работ по тематике информационной безопасности. Участник XX Научно-практической конференции «Комплексная защита информации».

E-mail: vadim.pif@gmail.com